LSU

POLICY STATEMENT 129
PHYSICAL SECURITY

PURPOSE

As an institution of higher education, the Louisiana State University A&M Baton Rouge Campus ("University" or "LSUAM") is charged with maintaining systems and data for administrative, academic, and research purposes. These assets are critical to the mission of the University, and physical security of these systems and data sets must be managed with a formalized Physical Security Policy.

The purpose of this policy is to define the required processes and activities involved in the management of assets as it pertains to physical security.

DEFINITIONS

Asset – A resource, process, product, information infrastructure, etc. whose loss or compromise could intangibly affect its integrity, availability, or confidentiality, or it could have a tangible dollar value. The loss or compromise of an asset could also affect an entity's ability to continue business. Examples of assets including, but are not limited to, equipment, software, algorithms, and data.

Data - Any information residing on the University IT Infrastructure or held on any other IT Infrastructure on behalf of the University. This data includes files, documents, messages in any format, including e-mail messages and posts made on any Social Media site maintained by/for the University or its units. All University data created and/or maintained by a User is also subject to this Policy, even if the data is created and/or stored on the User's own personal computer, smartphone, or other personal device.

IT Asset – For the purpose of these policies, IT Asset is a subset of Asset and specifically refers to hardware that have compute and storage capabilities (e.g., laptops, desktops, servers/virtual servers, mobile devices, etc.) and is utilized to store, process, access, and/or handle Data.

POLICY STATEMENT

A. Surveillance Cameras
   1. LSUAM shall establish processes and procedures for management of surveillance technology.
   2. LSUAM must identify a department responsible for overseeing surveillance technologies.

3. LSUAM shall define processes and procedures for reviewing and approving surveillance proposals.
4. LSUAM shall appropriately and clearly classify surveillance-related data as well as data retention policies for such data.

B. Physical Access Controls
1. LSUAM shall define standards that define what constitutes a secure area on campus as it relates to critical and/or sensitive IT assets.
2. LSUAM shall define a process for determining the elements involved in constructing a physical security perimeter to protect sensitive areas.
3. LSUAM shall define requirements to ensure that only authorized personnel are allowed access to controlled areas.

C. Facility Planning
1. LSUAM shall ensure aspects of physical security of IT assets to be held within a facility are included in the design for a new facility or upgrades to an existing one.
2. LSUAM shall ensure that requirements such as cooling, power, etc., are included in the design for a new facility or upgrades to an existing one.
3. LSUAM shall define guideless for the fire protection of data centers containing enterprise information assets, as all as any other areas classified as data centers by the University or departments.

STANDARDS

A. The Surveillance Cameras processes and procedures are outlined in LSU FASOP – LSUPD-02
B. The Physical Access Controls standards are outlined in Standard PS-129-ST-1.
C. The Facility Planning standards are outlined in Standard PS-129-ST-2.

EXCEPTIONS AND NON-COMPLIANCE

- Please refer PS-120-ST-4 for additional information related to exceptions.
- Please refer PS-120 for additional information related to Policies and Standards non-compliance.

REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	7/21/2023	Initial Draft	Information Technology Services